

to a personal security device and (2) encapsulates APDUs received from the personal security device into outgoing message packets and routes the outgoing message packets to the remote computer.

Urien describes a system for establishing communication between a PSD (smart card 2) and a remote computer system (remote server 4) over a network RI using a local client (PC terminal 1) as a host for the PSD. The local client includes a section for functionally connecting to a PSD interface (this section includes a reader 3) and the network and a section for functionally communicating over the network with the remote computer system.

PC terminal 1 comprises a client communications section for transmitting and receiving message packets over the network using a packet based communications protocol, since network RI may be the internet (Urien col. 2, lines 1-12). As shown in Urien's Fig. 1B, the client communications section is adapted for transmitting and receiving APDUs to and from smart card 2 through reader 3. Command and response APDUs are exchanged between smart card 2 and PC terminal 1 according to the ISO-7816 standard (col. 2, line 63, through col. 3, line 33).

However, Urien does not disclose that APDUs are communicated between smart card 2 and remote server 4. On the contrary, data exchanged between smart card 2 and remote server 4 are exchanged in two steps:

- the first step including exchanges of messages between smart card 2 and PC terminal 1 using APDUs; and
- the second step including exchanges of messages between PC terminal 1 and remote server 4 over network RI using a packet-based communications protocol.

Therefore, although not specified, PC terminal 1 may comprise a first data processing section for receiving incoming messages from remote server 4 using the client communications means and for separating encapsulated APDUs from the incoming messages, in case these incoming messages include such APDUs. PC terminal 1 may also comprise a second data processing section for encapsulating APDUs into outgoing message packets and routing the outgoing message packets to remote server 4 through the communications means. But, despite messages exchanged between PC terminal 1 and smart card 2 comprising APDUs, the APDUs exchanged between PC terminal 1 and smart card 2 are not the APDUs that are separated by PC terminal 1 from incoming messages received from remote server 4. Therefore, Urien differs from claim 1 in that the first data processing section is not suitable for routing those APDUs which are separated from incoming message packets to the PSD through the reader.

Urien describes in reference to Figs. 1B, 3, and 4, that the APDUs transferred to smart card 2 by PC terminal 1 are generated

by PC terminal 1 itself, in an APDU manager 102. Moreover, Urien does not describe how incoming APDUs from smart card 2 would be directly encapsulated by PC terminal 1 into message packets to be transferred to remote server 4. Therefore, Urien also differs from claim 1 in that the second data processing section is not suitable for encapsulating into outgoing message packets the APDUs received from smart card 2 by PC terminal 1.

In summary, Urien does not disclose effectuating a communications pipe between a PSD and a remote computer system over a network by: (1) directly encapsulating APDUs coming from the PSD interface of a client into outgoing messages sent to the remote computer system over the network and (2) directly routing to the PSD interface the APDUs desencapsulated by the client from messages coming from the remote computer system over the network.

DiGiorgio describes a system for establishing communication between a PSD (smart card 10) and a remote computer system (remote server 16) over a network that includes a local client (computer system 14) used as a host for the PSD. The local client has a section for functionally connecting to a PSD interface (this section includes a reader 12) and the network (between computer system 14 and remote server 16) and a section for functionally communicating over the network with the remote computer system. Computer system 14 has a client communications

section for transmitting and receiving message packets over the network using a packet based communications protocol (DiGiorgio col. 5, lines 47-56). The client communications section is adapted for transmitting and receiving APDUs to and from smart card 10 through reader 12 (col. 9, lines 1-6). The command APDU 100 depicted in Fig. 8A and the response APDU 101 depicted in Fig. 8B are exchanged between smart card 10 and computer system 14 (col. 9, lines 6-15). But no APDU is exchanged between smart card 10 and remote server 16. Therefore, the two-way challenge response authentication between smart card 10 and remote server 16, described in column 10, lines 24-35, does not describe smart card 10 and remote server 16 exchanging APDUs.

On the contrary, authentication messages exchanged between remote server 16 and smart card 10 are exchanged in two steps:

- the first step including exchanges of messages between remote server 16 and computer system 14 over the network using a packet based communications protocol; and

- the second step including exchanges of messages between computer system 14 and smart card 10 using APDUs.

Therefore, although not specified, computer system 14 may comprise a first data processing section for receiving incoming messages from remote server 16 using the client communications section and for separating encapsulated APDUs from the incoming

messages, in case these incoming messages include APDUs.

Computer system 14 may also comprise a second data processing section for encapsulating APDUs into outgoing message packets and routing the outgoing message packets to remote server 16 through the communications section.

However, despite messages exchanged between computer system 14 and smart card 10 comprising APDUs, the APDUs exchanged between smart card 10 and computer system 14 are not those APDUs separated by computer system 14 from incoming messages from remote server 16. Therefore, DiGiorgio differs from claim 1 in that the first data processing section is not suitable for routing those APDUs which are separated from incoming message packets to the PSD through reader 12.

Instead, according to what is described in column 9, it appears that the APDUs transferred to smart card 10 by computer system 14 are generated by computer system 14 itself. Moreover, nothing is described concerning incoming APDUs from smart card 10 that would be directly encapsulated by computer system 14 into message packets to be transferred to remote server 16. Therefore, DiGiorgio also differs from claim 1 in that the second data processing section is not suitable for encapsulating into outgoing message packets those APDUs which are received from smart card 10 through reader 12. Accordingly, DiGiorgio does not

disclose creating a communications pipe between a PSD and a remote computer system over a network by: (1) directly encapsulating APDUs coming from the PSD interface of a client into outgoing messages sent to the remote computer system over the network and (2) directly routing to the PSD interface APDUs desencapsulated by the client from messages coming from the remote computer system over the network.

The aim of the invention as defined by claim 1 is to overcome the problem of security within client terminals connected to a network, such as the Internet, by generating a communications pipe between a PSD and a secured remote computer system, so as to relocate the APDU interface and security mechanisms to the secured remote computer system. Urien and DiGiorgio do not describe a system that may achieve this goal.

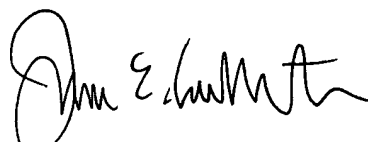
Accordingly, the Applicants respectfully submit that the applied references do not teach or suggest the above-noted subject matter defined by claim 1. Independent claims 12 and 17 similarly recite the above-described distinguishing feature of creating a communications pipe between a remote computer system and a PSD over a network by directly routing to a PSD interface APDUs desencapsulated by the client from messages coming from the remote computer system over the network. Therefore, allowance of

claims 1, 12, and 17 and all claims dependent therefrom is warranted.

In view of the above, it is submitted that this application is in condition for allowance and a notice to that effect is respectfully solicited.

If any issues remain which may best be resolved through a telephone communication, the Examiner is requested to telephone the undersigned at the local Washington, D.C. telephone number listed below.

Respectfully submitted,



James E. Ledbetter  
Registration No. 28,732

Date: January 18, 2006  
JEL/DWW/att

Attorney Docket No. L741.01103  
STEVENS DAVIS, MILLER & MOSHER, L.L.P.  
1615 L Street, N.W., Suite 850  
P.O. Box 34387  
Washington, D.C. 20043-4387  
Telephone: (202) 785-0100  
Facsimile: (202) 408-5200